UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/654,960	09/05/2003	Takashi Enami	242325US2	7967

22850 7590 11/09/2009

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, L.L.P.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
MAI, KEVIN S	

ART UNIT	PAPER NUMBER
2456	

NOTIFICATION DATE	DELIVERY MODE
11/09/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	Application No.	Applicant(s)	
	10/654,960	ENAMI ET AL.	
	Examiner	Art Unit	
	KEVIN S. MAI	2456	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 June 2009 and 14 April 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action has been issued in response to Applicant's Request for Continued Examination filed June 5, 2009.

2. Claims 1, 9, 11, 15, 17, 19-26 and 30 have been amended. Claims 1-30 have been examined and are pending.

Continued Examination Under 37 CFR 1.114

3. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submissions filed on April 14, 2009 and August 28, 2009 have been entered.

Response to Arguments

4. Applicant's arguments filed April 14, 2009 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claims 25 and 30 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Claim 25 recites the first image forming apparatus using the second password to determine whether to transfer the file to the document management server, however examiner was unable to find support for this limitation.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1-3, 5, 9-13, 15, 20, 21, 23, 24 and 26-30 are rejected under 35 U.S.C. 102(e) as being anticipated by US Pub. No. 2003/0101342 to Hansen (hereinafter "Hansen").

9. **As to Claim 1,** Hansen discloses **a file transfer system, comprising:**

a file management server comprising a web page configured to manage a transfer of files and to allow the files to be accessed subject to a first password through the webpage (Paragraph [0025] of Hansen discloses an information holding station located remotely from the printing station. This station includes a secure server to hold documents in storage and supply

documents for printing upon requests. Information holding station acts as a network printing manager to handle printing requests among one or more printing stations. Paragraph [0031] discloses password/login function permits confidential access to the printing system and paragraph [0033] discloses the secure server includes a website. Figure 1);

a file transmitting terminal configured to store a file and a second password for accessing the file, the second password being associated with the file (Paragraphs [0026]-[0027] of Hansen discloses computer workstation being used to send a document electronically to information holding station. Paragraph [0028] discloses pre-identifying the security key to be used for printing the document. Figure 1);

a file receiving terminal (Paragraph [0027] of Hansen discloses submitting a request to print a document at a printing station. Figure 1); **and**

a mobile terminal (Paragraph [0027] of Hansen discloses a mobile computing device. Figure 1),

wherein

said file management server, said file transmitting terminal, said file receiving terminal, and the mobile terminal are connected to each other via a network (Figure 1 of Hansen discloses all the components being in connected via a network communication link);

said file transmitting terminal is configured to transmit, to said file management server, the file and the second password as a part of an authentication condition for accessing the file, through the web page (Paragraphs [0026]-[0027] of Hansen discloses computer workstation being used to send a document electronically to information holding station. Paragraph [0028]

discloses pre-identifying the security key to be used for printing the document. Paragraph [0033] discloses the secure server includes a website);

said file management server is configured to store and to correlatingly manage the file and the second password transmitted from said file transmitting terminal (Paragraph [0027] of Hansen discloses a document being held at the server for printing. Wherein the document is accessed via a security key and paragraph [0028] discloses pre-identifying the security key. Thus the server holds the document and the key correlatingly);

said mobile terminal is configured to transfer an address of a particular file receiving terminal that is permitted to access the file, to said file management server through the web page (Paragraph [0027] of Hansen disclose the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer);

said file management server is configured to store and to correlatingly manage the address of said particular receiving terminal with the file (Paragraph [0027] of Hansen disclose the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer);

said file receiving terminal is configured to transmit to said file management server a request for transferring the file (Figure 6 of Hansen discloses the printer securely getting the print job from the server (310)); **and**

in response to the request transmitted by said file receiving terminal, if an address of said file receiving terminal and the address of the particular file receiving terminal transferred

by the mobile terminal are determined match, and if the request transmitted by said file receiving terminal is determined to include the second password, said file management server is configured to transfer the file to said file receiving terminal (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310)).

10. **As to Claim 2,** Hansen discloses the invention as claimed as described in claim 1 **wherein**

said authorization condition corresponding to said file is said second password for accessing said file (Paragraph [0027] of Hansen discloses a document being held at the server for printing. Wherein the document is accessed via a security key and paragraph [0028] discloses pre-identifying the security key)**; and**

said file management server is configured to, if a password transmitted with said request by said file receiving terminal matches said password transmitted by said file transmitting terminal, transmit said file to said file receiving terminal (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore

paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310)).

11. **As to Claim 3,** Hansen discloses the invention as claimed as described in claim 1. **wherein**

said authorization condition is one or more user IDs that are authorized to access said file (Paragraph [0027] of Hansen discloses the security key comprises a conventional password, digital signature or ID, or some other encryption system in which one or more passwords or signatures are used to create a unique identifier to permit access to the secure document only by the owner/operator of the unique identifier)**; and**

said file management server, is configured to, if a user ID transmitted with said request by said file receiving terminal is included in said one or more user IDs transmitted by said file transmitting terminal, transmit said file to said file receiving terminal (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Figure 6 discloses the printer securely getting the print job from the server (310)).

12. **As to Claim 5,** Hansen discloses the invention as claimed as described in claim 1. **wherein**

said file transmitting terminal is configured to transmit an effective period corresponding to said file (Paragraph [0029] of Hansen discloses time (duration, time of day, day of week, etc) can be used as a factor in determining whether to allow selective printing at printing station)**;**
said file management server is configured to store the corresponding effective period with said file (Paragraph [0029] of Hansen discloses time (duration, time of day, day of week, etc) can be used as a factor in determining whether to allow selective printing at printing station)**;**
and
said file management server is configured to, if the corresponding effective period has expired, prohibit said file from being transmitted (Paragraph [0029] of Hansen discloses time (duration, time of day, day of week, etc) can be used as a factor in determining whether to allow selective printing at printing station)**.**

13. **As to Claim 9,** Hansen discloses the invention as claimed as described in claim 1
wherein
said mobile terminal is configured to acquire the address of said file receiving terminal and to transmit the address to said file management server (Paragraph [0027] of Hansen disclose the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer)**;**
said file management server is configured to store the address of said file receiving terminal transmitted from said mobile terminal (Paragraph [0027] of Hansen disclose the mobile device transmits printing instructions which specify how, when and where the document will be

printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer)**; and**

said file management server is configured to, in response to said request for transmitting said file from said file receiving terminal, transmit the file to said file receiving terminal if the address of said file receiving terminal matches the stored address (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310))**.**

14. **As to Claim 10,** Hansen discloses the invention as claimed as described in claim 1**, wherein said file receiving terminal is configured to print or to store, in a recording medium, said file received from said file management server** (Figure 6 of Hansen discloses the printer securely getting the print job from the server and printing the document (310))**.**

15. **As to Claim 11,** Hansen discloses **a file management server connected to a file transmitting terminal, a file receiving terminal, and a mobile terminal via a network, comprising:**

a communication unit configured to exchange data with an external apparatus via said network (Paragraph [0027] of Hansen discloses a mobile computing device communicating with various apparatuses through a network. Figure 1);

a display unit configured to display a web page for transmitting files (Paragraph [0030] of Hansen discloses a user interface displaying a printing menu to enable communication with information holding station. Paragraph [0033] discloses the secure server utilizes a website);

a first storage unit configured to store a file and a second password as part of an authorization condition for accessing said file, the second password being associated with the file (Paragraphs [0026]-[0027] of Hansen discloses computer workstation being used to send a document electronically to information holding station. Paragraph [0028] discloses pre-identifying the security key to be used for printing the document. Figure 1);

a second storage unit configured to store an address of a particular file receiving terminal that is a to be allowed to access the file, the address being transmitted from the mobile terminal through the web page (Paragraph [0027] of Hansen disclose the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer);

a file transferring unit configured to, in response to a request for transferring said file stored in said first storage unit from said file receiving terminal, transfer said file to said file receiving terminal if an address of said file receiving terminal and the address of the particular file receiving terminal transmitted from the mobile terminal are determined to match, and if the request for transferring said file is determined to include the second

password is satisfied (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310))

16. **As to Claim 12,** Hansen discloses the invention as claimed as described in claim 11, **wherein**

said authorization condition corresponding to said file is said second password for accessing said file (Paragraph [0027] of Hansen discloses a document being held at the server for printing. Wherein the document is accessed via a security key and paragraph [0028] discloses pre-identifying the security key)**; and**

said file transferring unit is configured to, if a password transmitted with said request matches said password stored in said first storage unit, transfer said file to said file receiving terminal (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this

criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310)).

17. **As to Claim 13,** Hansen discloses the invention as claimed as described in claim 11 **wherein**

said authorization condition corresponding to said file is one or more user IDs (Paragraph [0027] of Hansen discloses the security key comprises a conventional password, digital signature or ID, or some other encryption system in which one or more passwords or signatures are used to create a unique identifier to permit access to the secure document only by the owner/operator of the unique identifier)**; and**

said file transferring unit is configured to, if a user ID transmitted with said request is included in said one or more user IDs stored in said first storage unit, transfer said file to said file receiving terminal (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Figure 6 discloses the printer securely getting the print job from the server (310)).

18. **As to Claim 15,** Hansen discloses the invention as claimed as described in claim 11 **wherein**

said first storage unit is configured to further store an effective period of said file (Paragraph [0029] of Hansen discloses time (duration, time of day, day of week, etc) can be used as a factor in determining whether to allow selective printing at printing station)**; and**

said file transfer unit is configured to, if the effective period of said file has expired, avoid transferring said file to said file receiving terminal (Paragraph [0029] of Hansen discloses time (duration, time of day, day of week, etc) can be used as a factor in determining whether to allow selective printing at printing station).

19. **As to Claim 20,** Hansen discloses **a file transfer method, comprising the steps of: displaying a web page configured to transfer and to receive files** (Paragraph [0030] of Hansen discloses a user interface displaying a printing menu to enable communication with information holding station. Paragraph [0033] discloses the secure server utilizes a website); **storing a file and a second password as part of an authorization condition for accessing the file transmitted by said file transfer terminal through the web page, the second password being associated with the file** (Paragraphs [0026]-[0027] of Hansen discloses computer workstation being used to send a document electronically to information holding station. Paragraph [0028] discloses pre-identifying the security key to be used for printing the document. Figure 1); **storing an address of a particular file receiving terminal that is allowed to access the file the address being transmitted from a mobile terminal through the web page** (Paragraph [0027] of Hansen disclose the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer);

receiving a request for transmitting said file designated from a file receiving terminal (Figure 6 of Hansen discloses the printer securely getting the print job from the server (310)); **and**

in response to the request, transmitting said file to said file receiving terminal if an address of said file receiving terminal and the address of the particular file receiving terminal match, and if the second password is satisfied (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310))

20. **As to Claim 21,** Hansen discloses **a computer-readable storage medium having embedded therein instruction, which when executed by a processor causes the processor to perform the method of:**

displaying a web page configured to transfer and to receive files (Paragraph [0030] of Hansen discloses a user interface displaying a printing menu to enable communication with information holding station. Paragraph [0033] discloses the secure server utilizes a website) **storing a file and a second password as part of an authorization condition for accessing the file transmitted by said file transfer terminal through the web page** (Paragraphs [0026]-[0027] of Hansen discloses computer workstation being used to send a document electronically

to information holding station. Paragraph [0028] discloses pre-identifying the security key to be used for printing the document. Figure 1);

storing an address of a particular file receiving terminal that is to be allowed to access the file the address being transmitted from a mobile terminal through the web page (Paragraph [0027] of Hansen disclose the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer);

receiving a request for transmitting said file designated from a file receiving terminal (Figure 6 of Hansen discloses the printer securely getting the print job from the server (310));

in response to the request, transmitting, said file to said file receiving terminal if an address of said file receiving terminal and the address of the particular file receiving terminal match, and if the second password is satisfied (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310))

21. **As to Claim 23,** Hansen discloses **a stored document management server connected to a first image forming apparatus, a second image forming apparatus, and a mobile terminal via a network, comprising:**

a communication unit configured to exchange data with said first and second image forming apparatuses via said network (Paragraph [0027] of Hansen discloses a mobile computing device communicating with various apparatuses through a network. Figure 1)**;**

a display unit configured to display a web page for transmitting stored documents (Paragraph [0030] of Hansen discloses a user interface displaying a printing menu to enable communication with information holding station. Paragraph [0033] discloses the secure server utilizes a website)**;**

a first storage unit configure to store a stored document and a second password as part of an authorization condition for accessing said stored document related to each other (Paragraphs [0026]-[0027] of Hansen discloses computer workstation being used to send a document electronically to information holding station. Paragraph [0028] discloses pre-identifying the security key to be used for printing the document. Figure 1)**;**

a second storage unit configure to store an address of a particular image forming apparatus that is to be allowed to access the stored document, the address being transmitted from the mobile terminal through the web page (Paragraph [0027] of Hansen disclose the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer)**; and**

a stored document transferring unit configured to, in response to a request for transferring said stored document stored in said first storage unit from said second image forming apparatus, transfer said stored document to said second image forming apparatus if an address of said second image forming apparatus and the address of the particular image

forming apparatus match, and if the second password is satisfied (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310))

22. **As to Claim 24,** Hansen discloses **an image forming system, comprising:**

a first image forming apparatus configured to manage a transfer of stored documents and to allow the stored documents to be accessed subject to a first password (Paragraph [0025] of Hansen discloses an information holding station located with the printing station. This station includes a secure server to hold documents in storage and supply documents for printing upon requests. Information holding station acts as a network printing manager to handle printing requests among one or more printing stations. Paragraph [0031] discloses password/login function permits confidential access to the printing system and paragraph [0033] discloses the secure server includes a website. Figure 1), **and to store a stored document and a second password for accessing the stored document, the second password being associated with the stored document** (Paragraph [0027] of Hansen discloses a document being held at the server for printing. Wherein the document is accessed via a security key and paragraph [0028] discloses pre-identifying the security key. Thus the server holds the document and the key correlatingly);

a user terminal (Paragraph [0027] of Hansen discloses a mobile computing device. Figure 1); **and**

a second image forming apparatus (Paragraph [0025] of Hansen discloses the secure server acts to hold documents in storage and communicates with one or more printing stations); **wherein**

said first image forming apparatus, said user terminal, and said second image forming apparatus are connected to each other via a network (Figure 1 of Hansen discloses all the components being in connected via a network communication link); **in response to a request from said user terminal, said first image forming apparatus is configured to, if the request from said user terminal is determined to include the second password, transmit said stored document and said second password as a part of an authorization condition for accessing the stored document to said second image forming apparatus** (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310)); **and**

said second image forming apparatus is configured to store said stored document and said second password associated with the stored document and, if a received request for printing said stored document is determined to include said second password, to print said

stored document (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310)).

23. **As to Claim 26,** Hansen discloses **an image forming apparatus connected with another image forming apparatus via a network, comprising:**
a communication unit configured to exchange data via said network, and, subject to a first password, to receive a stored document and a second password from said other image forming apparatus, the second password being associated with the stored document
(Paragraph [0025] of Hansen discloses an information holding station located with the printing station. This station includes a secure server to hold documents in storage and supply documents for printing upon requests. Information holding station acts as a network printing manager to handle printing requests among one or more printing stations. Paragraph [0031] discloses password/login function permits confidential access to the printing system and paragraph [0033] discloses the secure server includes a website. Figure 1. Paragraph [0027] of Hansen discloses a document being held at the server for printing. Wherein the document is accessed via a security key and paragraph [0028] discloses pre-identifying the security key. Thus the server holds the document and the key correlatingly);

a storage configured to store the stored document and the second password associated with the stored document as part of an authorization condition for accessing said stored document received from said other image forming apparatus (Paragraph [0027] of Hansen discloses a document being held at the server for printing. Wherein the document is accessed via a security key and paragraph [0028] discloses pre-identifying the security key. Thus the server holds the document and the key correlatingly)**;**

an operations input unit (Paragraph [0030] of Hansen discloses a user interface displaying a printing menu to enable communication with information holding station)**; and**

an image forming unit configured to, in response to reception of a request for printing said stored document, if the request for printing said stored document includes the second password, print said stored document (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server and printing it (310))**.**

24. **As to Claim 27,** Hansen discloses the invention as claimed as described in claim 26**, wherein**

said image forming apparatus is further connected to a user terminal via said network (Paragraph [0027] of Hansen discloses a mobile computing device. Figure 1)**; and**

said communication unit is configured to, in response to a transfer request from said user terminal, if said transfer request satisfies said authorization condition, transmit said stored document and said authorization condition stored in said storage unit to a destination (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310)).

25. **As to Claim 28,** Hansen discloses the invention as claimed as described in claim 27, **wherein said transfer request includes said destination, the second password as said authorization information for accessing said stored document, and a registration code of said stored document that said communication unit has received from said user terminal via said network** (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310)).

26. **As to Claim 29,** Hansen discloses the invention as claimed as described in claim 27, **wherein said transfer request includes said destination, said authorization condition for accessing said stored document, and a registration code of said stored document that are input by said operations input unit** (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310)).

27. **As to Claim 30,** Hansen discloses **an image forming apparatus connected with a stored document management server and a user terminal via a network, comprising: a communication unit configured to exchange data via said network and, subject to a first password, to transmit a stored document and a second password to the stored document management server, the second password being associated with the stored document** (Paragraph [0025] of Hansen discloses an information holding station located with the printing station. This station includes a secure server to hold documents in storage and supply documents for printing upon requests. Information holding station acts as a network printing manager to handle printing requests among one or more printing stations. Paragraph [0031] discloses password/login function permits confidential access to the printing system and paragraph [0033] discloses the secure server includes a website. Figure 1. Paragraph [0027] of Hansen discloses a

document being held at the server for printing. Wherein the document is accessed via a security key and paragraph [0028] discloses pre-identifying the security key. Thus the server holds the document and the key correlatingly);

a storage unit configured to store a stored document and the second password associated with the stored document as a part of an authorization condition for accessing said stored document (Paragraph [0027] of Hansen discloses a document being held at the server for printing. Wherein the document is accessed via a security key and paragraph [0028] discloses pre-identifying the security key. Thus the server holds the document and the key correlatingly);

and

an image forming unit configured to print said stored document (Figure 6 of Hansen discloses the printer securely getting the print job from the server and printing it (310));

wherein

said communication unit is configured to, in response to reception of a request for transmitting said stored document from said user terminal, if the request for transmitting said stored document is determined to include the second password, transmit said stored document and second password said authorization condition to said stored document management server (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this

criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310)).

Claim Rejections - 35 USC § 103

28. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

29. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

30. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

31. Claims 22, 25 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hansen.

32. **As to Claim 22,** Hansen discloses **an image forming system, comprising:**

a stored document management server comprising a web page configured to manage a transfer of stored documents and to allow the stored documents to be accessed subject to a first password through the web page (Paragraph [0025] of Hansen discloses an information holding station located remotely from the printing station. This station includes a secure server to hold documents in storage and supply documents for printing upon requests. Information holding station acts as a network printing manager to handle printing requests among one or more printing stations. Paragraph [0031] discloses password/login function permits confidential access to the printing system and paragraph [0033] discloses the secure server includes a website. Figure 1)**;**

a first [image forming] apparatus configured to store a stored document and a second password for accessing the stored document (Paragraphs [0026]-[0027] of Hansen discloses computer workstation being used to send a document electronically to information holding station. Paragraph [0028] discloses pre-identifying the security key to be used for printing the document. Figure 1)**;**

a second image forming apparatus (Paragraph [0027] of Hansen discloses submitting a request to print a document at a printing station. Figure 1)**; and**

a mobile terminal (Paragraph [0027] of Hansen discloses a mobile computing device. Figure 1),

wherein

said stored document management server, said first image forming apparatus, and said second image forming apparatus, and said mobile terminal are connected to each other via a network (Figure 1 of Hansen discloses all the components being in connected via a network communication link)**;**

said first image forming apparatus is configured to transmit, to said stored document management server, said stored document and the second password as a part of an authorization condition for accessing said stored document, through the web page (Paragraphs [0026]-[0027] of Hansen discloses computer workstation being used to send a document electronically to information holding station. Paragraph [0028] discloses pre-identifying the security key to be used for printing the document. Paragraph [0033] discloses the secure server includes a website)**;**

said stored document management server is configured to store and to correlatingly manage the transmitted stored document and the second password transmitted form the first image forming apparatus (Paragraph [0027] of Hansen discloses a document being held at the server for printing. Wherein the document is accessed via a security key and paragraph [0028] discloses pre-identifying the security key. Thus the server holds the document and the key correlatingly)**;**

said mobile terminal is configured to transfer an address of a particular image forming apparatus that is permitted to access the stored document, to said stored document management server through the web page (Paragraph [0027] of Hansen disclose the mobile device transmits printing instructions which specify how, when and where the document will be

printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer);

said stored document management server is configured to store and to correlatingly manage the address of said particular image forming apparatus with the stored document (Paragraph [0027] of Hansen disclose the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer);

said second image forming apparatus is configured to transmit to said stored document management server a request for transferring the stored document (Figure 6 of Hansen discloses the printer securely getting the print job from the server (310));

and

in response to the request transmitted by the second image forming apparatus, if an address of said second image forming apparatus and the address of the particular image forming apparatus match, and if the second password is satisfied, said stored document management server, is configured to transfer the stored document to said second image forming apparatus (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310)).

Hansen does not explicitly disclose the first apparatus being **image forming.**

However, Honma discloses this. Column 17 lines 13-30 of Honma disclose a user being able to use an original image forming apparatus to access another image forming apparatus to obtain a document to print out on the original image forming apparatus.

It would have been obvious to one of ordinary skill in the art at the time of invention to combine the printing system as disclosed by Hansen, with having one image forming apparatus transfer to another as disclosed by Honma. One of ordinary skill in the art would have been motivated to combine to apply simple substitution of one known element for another to obtain predictable results. Honma discloses it is well known in the art to have one image forming apparatus provide a document to another image forming apparatus. Hansen discloses obtaining the document information from a computer work station. Thus it would have been simple substitution of one known element for another to implement such a feature in Hansen.

33. **As to Claim 25,** Hansen discloses **an image forming system, comprising: a first image forming apparatus configured to manage a transfer of stored documents and to allow the stored documents to be accessed subject to a first password** (Paragraph [0025] of Hansen discloses an information holding station located with the printing station. This station includes a secure server to hold documents in storage and supply documents for printing upon requests. Information holding station acts as a network printing manager to handle printing requests among one or more printing stations. Paragraph [0031] discloses password/login function permits confidential access to the printing system and paragraph [0033] discloses the secure server includes a website. Figure 1**), and to store a stored document and a second password for accessing the stored document, the second password being associated with the**

stored document (Paragraph [0027] of Hansen discloses a document being held at the server for printing. Wherein the document is accessed via a security key and paragraph [0028] discloses pre-identifying the security key. Thus the server holds the document and the key correlatingly);

a stored document management server (Paragraph [0025] of Hansen discloses an information holding station located remotely from the printing station. This station includes a secure server to hold documents in storage and supply documents for printing upon requests. Information holding station acts as a network printing manager to handle printing requests among one or more printing stations. Paragraph [0031] discloses password/login function permits confidential access to the printing system and paragraph [0033] discloses the secure server includes a website. Figure 1);

a user terminal (Paragraph [0027] of Hansen discloses a mobile computing device. Figure 1);

and

a second image forming apparatus (Paragraph [0025] of Hansen discloses the secure server acts to hold documents in storage and communicates with one or more printing stations);

wherein

said first image forming apparatus, said stored document management server, said user terminal, and said second image forming apparatus are connected each other via a network (Figure 1 of Hansen discloses all the components being in connected via a network communication link);

in response to a request from said user terminal, said first image forming apparatus is configured to, if the request from said user terminal is determined to include said second password, transmit said stored document and said second password as part of an

authorization condition to said stored document management server (Paragraphs [0026]-[0027] of Hansen discloses computer workstation being used to send a document electronically to information holding station. Paragraph [0028] discloses pre-identifying the security key to be used for printing the document. Paragraph [0033] discloses the secure server includes a website)**;**

said stored document management server is configured to store said stored document and said second password (Paragraph [0027] of Hansen discloses a document being held at the server for printing. Wherein the document is accessed via a security key and paragraph [0028] discloses pre-identifying the security key. Thus the server holds the document and the key correlatingly)**; and,**

in response to a request for transmitting said stored document from said second image forming apparatus, said stored document management server is configured to, if the request for transmitting said stored document is determined to include the second password, transmit said stored document to said second image forming apparatus (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310))**; and**

said second image forming apparatus is configured to print said stored document transmitted from said stored document management server (Figure 6 of Hansen discloses the printer securely getting the print job from the server and printing it (310)).

Hansen does not explicitly disclose the first apparatus being **image forming.**

However, Honma discloses this. Column 17 lines 13-30 of Honma disclose a user being able to use an original image forming apparatus to access another image forming apparatus to obtain a document to print out on the original image forming apparatus.

Examiner recites the same rationale to combine used in claim 22.

34. Claims 6-8 and 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hansen and further in view of US Pat. No. 6785812 to Botham, Jr. et al. (hereinafter "Botham").

35. **As to Claim 6,** Hansen discloses the invention as claimed as described in claim 5. Hansen does not explicitly disclose**, wherein said file management server is configured to, if the corresponding effective period has expired, delete said file**

However, Botham discloses this. Column 4 lines 34-36 of Botham discloses destroying a document once its allotted lifetime has expired.

It would have been obvious to one of ordinary skill in the art at the time of invention to combine the invention of claim 5 as disclosed by Hansen, with deleting a file after a period as disclosed by Botham. One of ordinary skill in the art would have been motivated to combine to apply a known technique to a know device ready for improvement to yield predictable results. Paragraph [0029] of Hansen discloses time (duration, time of day, day of week, etc) can be used

as a factor in determining whether to allow selective printing at printing station. Accordingly it would have been obvious to implement deleting the file after the time has expired, since it is seen to be a known technique used in view of utilizing time as a factor in printing.

36. **As to Claim 7,** Hansen discloses the invention as claimed as described in claim 1**.** Hansen does not explicitly disclose **wherein**

said file transmitting terminal is configured to transmit an effective number of transfers corresponding to said file;

said file management server is configured to store the corresponding effective number of transfers with said file; and

said file management server is configured to, if the number of transfers of said file reaches the corresponding effective number of transfers, prohibit said file from being transmitted.

However, Botham discloses this (Column 2 lines 45-55 of Botham disclose being able define control characteristics, including allowing a document to only be viewed or printed a maximum number of times. Then based on purpose of setting a maximum number of times a document may be printed it is inherent that when a file reaches the effective number, it will no longer be distributed)

It would have been obvious to one of ordinary skill in the art at the time of invention to combine the system of claim 1 as disclosed by Hansen, with having a maximum number of times a document may be printed as disclosed by Botham. One of ordinary skill in the art would have been motivated to combine to make document distribution more secure and controllable (column 2 lines 18-65 of Botham).

37. **As to Claim 8,** Hansen-Botham discloses the invention as claimed as described in claim 7, **wherein said file management server is configured to, if the number of transfers of said file reaches the corresponding effective number of transfers, delete said file** (Column 2 lines 45-55 of Botham disclose being able define control characteristics, including allowing a document to only be viewed or printed a maximum number of times. Thus it is seen that when a document has been viewed/printed the maximum number of times it is essentially no longer accessible, thus it would be obvious to delete the document in order to preserve space on the file management server)**.**

Examiner recites the same rationale to combine used in claim 7.

38. **As to Claim 16,** Hansen discloses the invention as claimed as described in claim 15. Hansen does not explicitly disclose**, wherein said file transferring unit is configured to, if the effective period of said file has expired, delete said file**

However, Botham discloses this. Column 4 lines 34-36 of Botham discloses destroying a document once its allotted lifetime has expired**.**

Examiner recites the same rationale to combine used in claim 6.

39. **As to Claim 17,** Hansen discloses the invention as claimed as described in claim 11**.** Hansen does not explicitly disclose **wherein**

said first storage unit is configured to further store an effective number of transfers of said file; and

said file transfer unit is configured to, if the number of transfers of said file reaches the effective number stored in said first storage unit, avoid transferring said file to said file receiving terminal.

However, Botham discloses this (Column 2 lines 45-55 of Botham disclose being able define control characteristics, including allowing a document to only be viewed or printed a maximum number of times. Then based on purpose of setting a maximum number of times a document may be printed it is inherent that when a file reaches the effective number, it will no longer be distributed)

Examiner recites the same rationale to combine used in claim 7.

40. **As to Claim 18,** Hansen-Botham discloses the invention as claimed as described in claim 17, **wherein said file transferring unit is configured to, if the number of transfers of said file reaches the effective number, delete said file** (Column 2 lines 45-55 of Botham disclose being able define control characteristics, including allowing a document to only be viewed or printed a maximum number of times. Thus it is seen that when a document has been viewed/printed the maximum number of times it is essentially no longer accessible, thus it would be obvious to delete the document in order to preserve space on the file management server).

Examiner recites the same rationale to combine used in claim 7.

41. Claims 4, 14 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hansen and further in view of US Pat. No. 6233618 to Shannon (hereinafter "Shannon").

42. **As to Claim 4,** Hansen discloses the invention as claimed as described in claim 1. Hansen does not explicitly disclose **wherein**

said authorization condition is the membership of a group that is authorized to access said file; and

said file management server is configured to, if a user ID transmitted with said request by said file receiving terminal is a member of said group, transmit said file to said file receiving terminal.

However, Shannon discloses this. Column 7 lines 58-68 of Shannon disclose a user of a particular group being restricted from viewing particular pages.

It would have been obvious to one of ordinary skill in the art at the time of invention to combine the system of claim 1 as disclosed by Hansen, with using membership of a group as the authorization condition as disclosed by Shannon. One of ordinary skill in the art would have been motivated to combine to improve access and control capabilities (column 3 lines 35-45 of Shannon).

43. **As to Claim 14,** Hansen discloses the invention as claimed as described in claim 11. Hansen does not explicitly disclose **further comprising a third storage unit configured to store a group name and user IDs of group members;**

wherein

said authorization condition stored in said first storage unit is said group name; and

said file transferring unit is configured to, if a user ID transmitted with said request is included in said group members, transfer said file to said file receiving terminal.

However, Shannon discloses this. Column 7 Table 1 discloses a storage associating Clients with their groups. Column 7 lines 58-68 of Shannon disclose a user of a particular group being restricted from viewing particular pages

Examiner recites the same rationale to combine used in claim 4.

44. **As to Claim 19,** Hansen-Shannon discloses the invention as claimed as described in claim 14 **wherein**

said second storage unit is configured to store the address of said file receiving terminal transmitted from the mobile terminal (Paragraph [0027] of Hansen disclose the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer)**, and**

said file transferring unit is configured to, in response to the request for transferring said file, said request transmitted from said file receiving terminal, only if the address of said file receiving terminal matches an address stored in said second storage unit, transmit said file to said file receiving terminal (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310))**.**

Conclusion

45. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US 5835922 A - Document processing apparatus and method for inputting the requirements of a reader or writer and for processing documents according to the requirements to Shima; Yoshihiro et al.

US 6914687 B1 - Data processing apparatus and image recording apparatus, method for controlling data processing apparatus and method for controlling image recording apparatus, and storage medium to Hosoda; Yuichi et al.

US 20030076526 A1 - Method and apparatus for printing documents using a document repository in a distributed data processing system to Gopalan, Prabhakar

US 6931432 B1 - Data transmission apparatus and method with control feature for transmitting data or transmitting a storage location of data to Yoshida; Hiroyoshi

US 7190475 B2 - Method for providing a print and apparatus to Nomoto; Tetsushi

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KEVIN S. MAI whose telephone number is (571)270-5001. The examiner can normally be reached on Monday through Friday 7:30 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Bunjob Jaroenchonwanit can be reached on 571-272-3913. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/K. S. M./
Examiner, Art Unit 2456

/Bunjob Jaroenchonwanit/

Supervisory Patent Examiner, Art Unit 2456